REMARKS

Claims 1-16 are all the claims pending in the application.

I. Objections to the Specification

The Examiner has objected to the specification for the reasons set forth on pages 2-3 of the Office Action. Applicants have amended the specification in a manner to overcome the Examiner's objections. Applicants note that additional editorial changes have also been made to the specification and abstract for grammatical and general readability purposes. No new matter has been added.

II. Claim Rejections under 35 U.S.C. § 102

Claims 1-3, 6-14 and 16 have been rejected under 35 U.S.C. § 102(e) as being anticipated by Nagamasa et al. (U.S. 2004/0177215).

Claim 1, as amended, is drawn to a semiconductor memory card comprising a tamper resistant module and a nonvolatile memory, wherein the tamper resistant module includes: an internal memory having a usage area used by a <u>program</u> stored in the tamper resistant module; and a <u>processing unit</u> including a <u>virtual machine</u> and an <u>operation system</u>, the <u>program being an application executed by the virtual machine</u>. Applicants respectfully submit that Nagamasa does not disclose or suggest at least the above-noted features recited in claim 1.

Regarding Nagamasa, Applicants note that this reference discloses the use of a multimedia card 110 which includes an IC card chip 150, a flash memory chip (i.e., non-volatile memory) 130, and a controller chip 120 (see Fig. 22 and paragraph [0042]). As shown in Fig. 26 of Nagamasa, the IC card chip 150 includes a CPU 158, a ROM 159, a RAM 160, and an

EEPROM 162 (see paragraph [0043]). As explained in Nagamasa, the EEPROM 162 is used for storing data including a program (see Fig. 26 and paragraph [0043]).

In the Office Action, the Examiner has taken the position that, in Nagamasa, the program stored on the EEPROM 162 of the IC card chip corresponds to the "program" of claim 1, and that the controller chip 120 corresponds to the "processing unit" of claim 1 (see Office Action at page 3).

As indicated above, however, Applicants note that claim 1 has been amended herein so as to recite that the processing unit includes a virtual machine and an operation system, the program being an application executed by the virtual machine.

Regarding the above-noted claim language, as well as the Examiner's above-noted correspondence between the claimed features and Nagamasa, Applicants respectfully submit that the controller chip 120 of Nagamasa clearly does not include a virtual machine and an operation system, and further, that the program on the EEPROM 162 is clearly not a program that is executed by a virtual machine included in the controller chip 120.

As such, Applicants respectfully submit that Nagamasa does not disclose, suggest or otherwise render obvious at least the above-noted feature set forth in amended claim 1 which recites that the processing unit includes a virtual machine and an operation system, the program being an application executed by the virtual machine. Accordingly, Applicants submit that claim 1 is patentable over Nagamasa, an indication of which is kindly requested.

In addition, Applicants note that claim 1 also recites that when requested by the program, the processing unit is operable to (i) assign an area in the nonvolatile memory to the program, and (ii) generate, on the internal memory of the tamper resistant module, access information for the assigned area, the usage area and the assigned area composing a total area for use by the program. Applicants respectfully submit that Nagamasa also does not disclose or suggest this feature of claim 1.

In particular, regarding the relationship between the flash memory chip 130, the IC card chip 150, and the controller chip 120, Applicants note that Nagamasa discloses that the flash memory chip 130 includes an area 2110 (which includes areas 2111-2116) for storing information which allows the controller chip 120 to manage the IC card chip 150 (see Fig. 21 and paragraph [0051]).

For example, as explained in Nagamasa, if security related data of a large size cannot be transmitted in a lump to the IC card chip 150 from the host apparatus 220, then the controller chip 120 selects the access to the flash memory chip 130 and temporarily stores the data into a security process buffer area 2114 having a large enough capacity (see paragraph [0052]). The controller chip 120 then divides the data into a size in which the data can be transmitted to the IC card chip 150, reads out the divided data from the flash memory chip 130, and transmits the divided data to the IC card chip 150 step by step (see paragraph [0052]).

Further, in Nagamasa, Applicants note that a security process is carried out when content is distributed from a contents provider 2310 to a user of the multimedia card 110 (see Fig. 23 and paragraphs [0054] and [0055]). Regarding this security process of Nagamasa, Applicants note that the process described in paragraph [0055] is a standard authentication process that is utilized in electronic payment services, and involves a verification routine that is carried out by a host apparatus 220 that communicates with the multimedia card 110 and the content provider 2310, and encryption/decryption of the content (see lines 12-41 of paragraph [0055], with the received content being written into the flash memory 130 and retrieved by the user (see lines 12-56 of paragraph [0055]).

In the Office Action, Applicants note that the Examiner has pointed to the above-described paragraph [0051] of Nagamasa as allegedly disclosing that the processing unit is operable to assign an area in the nonvolatile memory to a program, and has pointed to the above-described paragraph [0055] of Nagamasa as allegedly disclosing that the processing unit is operable to generate, on the internal memory of the tamper resistant module, access information for the assigned area, the usage area and the assigned area composing a total area for use by the program (see Office Action at pages 3-4).

Based on the Examiner's reliance on paragraphs [0051] and [0055] of Nagamasa, it appears as though the Examiner is taking the position that the buffer area 2114 of the flash memory chip 130 corresponds to the "assigned area" of the nonvolatile memory.

Regarding this position, Applicants note that while the controller chip 120 causes data that is to be transferred to the IC card chip 150 to be temporarily stored in the buffer area 2114 of the flash memory chip 130 (see paragraph [0051]), that the controller chip 120 does <u>not</u> function so as to assign the buffer area 2114 to a program when requested by the program. As such, Applicants respectfully submit that Nagamasa does not disclose the feature recited in claim 1 which sets forth that "when requested by the program, the processing unit is operable to (i) assign an area in the nonvolatile memory to the program".

Moreover, regarding the above-noted feature which indicates that the processing unit is operable to <u>generate</u>, on the internal memory of the <u>tamper resistant module</u>, <u>access information for the assigned area</u>, the usage area and the assigned area composing a total area for use by the program, Applicants initially note that it is not clear from the Examiner's reliance on paragraph [0055] of Nagamasa what information the Examiner believes corresponds to the "access information for the assigned area", as recited in claim 1.

In this regard, Applicants respectfully submit that the security process disclosed in paragraph [0055] of Nagamasa includes absolutely no disclosure or suggestion of the controller chip 120 (which the Examiner indicated corresponds to the "processing unit" of claim 1) having the ability to generate on a tamper resistant module <u>access information</u> for the buffer area 2114 (which the Examiner indicated corresponds to the "assigned area" of claim 1), and does not in any way disclose that the usage area of the <u>internal memory</u> and the <u>assigned area</u> of the nonvolatile memory compose a <u>total area for use by the program</u>.

In view of the foregoing, Applicants respectfully submit that Nagamasa does not disclose, suggest or otherwise render obvious all of the features recited in amended claim 1. Accordingly, Applicants submit that claim 1 is patentable over Nagamasa; an indication of which is kindly requested. Claims 3 and 6-14 depend from claim 1 and are therefore considered patentable at least by virtue of their dependency.

Regarding claim 16, Applicants note that this claim has been amended so as to recite that the tamper resistant module includes: an internal memory having a usage area used by an application stored in the tamper resistant module; a virtual machine; and an operation system, the application being executable by the virtual machine, and the controlling program is operable to (i) assign an area in the nonvolatile memory to the application, and (ii) generate, on the internal memory of the tamper resistant module, access information for the assigned area, the usage area and the assigned area composing a total area for use by the application.

For at least similar reasons as discussed above with respect to claim 1, Applicants respectfully submit that Nagamasa does not disclose, suggest or otherwise render obvious the above-noted combination of features recited in claim 16. Accordingly, Applicants submit that claim 16 is patentable over Nagamasa, an indication of which is kindly requested.

III. Claim Rejections under 35 U.S.C. § 103(a)

A. . Claims 4 and 5 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Nagamasa et al. in view of Madoukh (U.S. 2001/0019614).

Claims 4 and 5 depend from claim 1. Applicants submit that Madoukh fails to cure the deficiencies of Nagamasa et al., as discussed above, with respect to claim 1. Accordingly, Applicants submit that claims 4 and 5 are patentable at least by virtue of their dependency.

B. Claim 15 has been rejected under 35 U.S.C. § 103(a) as being unpatentable over Nagamasa et al. in view of Deo et al. (U.S. 5,721,781).

Regarding claim 15, Applicants note that this claim has been amended so as to depend from claim 1. In this regard, Applicants submit that Deo fails to cure the deficiencies of Nagamasa et al., as discussed above, with respect to claim 1. Accordingly, Applicants submit that claim 15 is patentable at least by virtue of its dependency.

IV. Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited.

If any points remain in issue which the Examiner feels may best be resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,

Hiromi EBARA et al.

By: Kenneth W. Fields
Kenneth W. Fields
Registration No. 52,430
Attorney for Applicants

KWF/ra
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
December 4, 2007